USAID Open Source Briefing

Tony Stanco, Esq., Associate Director
Cyber Security Policy & Research Institute
George Washington University
Washington, DC USA
http://www.cpi.seas.gwu.edu
stanco@seas.gwu.edu
202-994-5513
The Center for Open Source in Government
http://www.eGovOS.org

The Institute

- **Cyber Security Policy & Research Institute (CSPRI)**
  - Founded 1993
  - Focus on Information Technology Security, Policy, and Research
- **Recent Research Topics**
  - Security-Enhanced Linux
  - NIAP/Common Criteria Certification of Linux and PKI/CAC
  - Network Intrusion Detection Systems
  - Public Key Infrastructure (PKI)
  - Secure Object Infrastructure/Mobile Agent Security
  - Wireless IEEE 802.11a and IEEE 802.11b Security

Open Source in Government Conferences

- **GW/CSPRI co-organized International Open Source in Government Conference October 16-18, 2002 with UN and World Bank**
  - 400 participants from 30 countries -- like EU, Germany, UK, France, Canada, Mexico, Denmark, India, China
- **GW/CSPRI organizing U.S./EU Open Source in Government Conference March 17-19, 2003**
  - for federal, state, military senior IT officials
  - confirmed presenters include DISA, DARPA, NSA, Census, NIST, GSA, State of Rhode Island, State of Utah, IBM, SUN, SAIC

Open Source

PITAC

- Open Source Software (OSS) interest at the highest levels of government
- PITAC October 2000 Report on Developing Open Source Software to Advance High End Computing
  - ”The PITAC believes the open source development model represents a viable strategy for producing high quality software through a mixture of public, private and academic partnerships”
  - ”By its very nature, this approach offers government the additional promise of leveraging its software research investments with expertise in academia and the private sector”

PITAC (2)

Findings:

- The Federal government needs to participate and invest in the development, support, distribution, and maintenance of OSS
- Security advantages of Open Source Software development efforts over the traditional proprietary development model

PITAC (3)

PITAC RECOMMENDATIONS:

1. Federal government should aggressively encourage the development of Open Source Software for high end computing
2. A “level playing field” must be created within the government procurement process to facilitate Open Source development

Congressional Interest

- May 2002, Congressional staffers were briefed on IT policy and Open Source Software by a group consisting of:
  - Grant Wagner (NSA),
  - Lisa Nyman (Census),
  - Douglas Maughan (DARPA),
  - Terry Bollinger (MITRE, author of the MITRE report)
  - Tony Stanco (George Washington University).

NSA's Security Enhanced Linux (SELinux) Project

- Project run by Grant M. Wagner, Information Assurance Research Group, Secure Systems Research Office

- Project Strategy
  - Build prototype system that addresses critical DOD/IC problems
  - Improve security of available systems
  - Demonstrate reduced vulnerability
  - Leverage growing popularity of Linux
  - Open source provides reference implementation

MITRE Report

- Report for Office of Secretary of Defense and DISA
- Publicly released October 28, 2002
  - **http://www.eGovOS.org/**

- The main conclusion is that open source software plays a critical role in the DOD, and that its use is especially critical for areas such as enterprise security, infrastructure support, research, and development.

- Surprisingly, one of the areas that would be most severely damaged by a ban on using Open Source is security, since many of the most reliable systems and most powerful security analysis tools are Open Source.

MITRE Report Recommendations

- Enable more use of Open Source:
  - Develop a "Generally Recognized As Safe" (GRAS) list of widely used, commercially supported Open Source Software with known security track records.
  - Develop distinct usage policies for four areas: Infrastructure, Development, Security, Research
  - Encourage use of commercial Open Source use to maintain cost/quality/security competition.
    - Use open source as a competitive tool for lowering total costs

Other Countries

- UK Cabinet Report called, "Open Source Software: Use Within the UK Government" predicts that within five years, 50% of the software used for the infrastructure market could be taken by Open Source Software
- January 2002, the Central Procurement Office of the Korean Government decided to put Linux and Open Source office products on the computers of 120,000 government employees
- Most countries are seriously looking at Open Source in one form or another -- EU, Germany, France, Canada, India, China, Mexico, Brazil, Spain, etc.

Open Source Software

- **Linux: Unix-Like Operating System**
  - Started 1992 by Linus Torvalds
  - Contains no Proprietary Code
  - Significant Server and Internet Presence
  - Significant Vendor Buy-in and Commercialization
- **Open-Source Model**
  - Powerful Development Model
  - No Traditional Vendor
  - GNU General Public License (GPL)

Open Source Benefits

- Reduced development costs
- Standards based reference implementations
- Faster implementations
- Enhanced Security
- Increased interoperability
- No lock-in or reliance to single, proprietary vendor
  - Allows Competitive bids on outyear Contracts for service and maintenance
- Faster response time for bug fixes through peer review

Open Source Security

- Security benefits for Federal Information Technology systems
  - Wide peer review
  - Rapid patching
  - Variability and user customization possible
  - Defensive/Offensive bug fixes for military
    - fix own bugs, leave vulnerabilities in others

Open Source Cost Savings

- Mostly unfunded project that could not be done with proprietary software costs
- An estimated cost savings of $311,000 using Open Source in the FedStats project reported by Census
- Project won CIO Council Award

	Proprietary	Open Source	Percent cost reduction
Operating system and hardware	80,000	30,000	-67%
Web server	3,000	0	-100%
Database	80,000	12,000	-85%
Search software	195,000	5,000	-97%

Open Source Market Share

- 27% of Server Sales (IDC 2000)
- 29.6% of Web Servers (Netcraft 2001)
- 48.1% of Developers Plan to Use Linux (Evans Data 2001)

Open Source Performance

- Linux/Samba 100% faster than than Windows 2000 Server (PC Magazine 2002)
- Linux/TUX faster than Windows 2000/IIS on Wide Range of Dell Servers (SPEC Consortium 2001)
- Linux Pipes faster than Windows 2000 and XP (IBM 2001)

Open Source Reliability

- Three Fuzz Studies: Fuzz (1990), Fuzz Revisited (1995), Windows (2000)
- Unix Study (1995)
  - GNU/Linux best: 6%/9% Failure Rates
  - Best Commercial Unix (HP-UX): 18% Failure Rate
  - All GNU/Linux Problems Have Been Corrected (Scott Maxwell)
- Windows NT/2000 Study (2000)
  - Windows NT/2000: 45% Failure Rate
  - Windows NT/2000 Messaging; 100% Failure Rate
- GNU/Linux Compares Favorably against Unix and Windows

IT Vendor Buy-in

- IBM spent $1 billion on Linux last year, and it is using Linux to power all of its major product lines, right up to its mainframes.
- Recently, SUN, HP/Compaq, Apple, DELL and Oracle have announced that they are adding Open Source solutions to their product lines

Research Compendium

- “Why Open Source Software/Free Software (OSS/FS)? Look at the Numbers!”
- By David A. Wheeler
- http://www.dwheeler.com/oss_fs_why.html
- Excellent starting point for information

USAID Open Source Briefing

Tony Stanco, Esq., Associate Director
Cyber Security Policy & Research Institute
George Washington University
Washington, DC USA
http://www.cpi.seas.gwu.edu
stanco@seas.gwu.edu
202-994-5513
The Center for Open Source in Government
http://www.eGovOS.org